Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Acer Service Corporation (Organization)
Decision number (file number)	P2017-ND-36 (File #003052)
Date notice received by OIPC	June 3, 2016
Date Organization last provided information	September 21, 2016
Date of decision	March 1, 2017
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization's principal place of business is Texas, United States. It is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in this incident: • name, • address, • payment card information (credit card number, expiration date, and CVV number). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's ecommerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On April 26, 2016, the Organization discovered that during the testing and roll out of the Organization's ecommerce website the debugging mode was inadvertently turned on, which stored payment card transaction data in plain text. An unauthorized third party subsequently exploited a misconfiguration in the Organization's ecommerce servers to gain access to and acquire the information at issue. • The intrusion potentially exposed the personal information of individuals who made purchases using the ecommerce site between May 12, 2015, and April 28, 2016. • To date the perpetrator has not been apprehended.
Affected individuals	A total of 35,000 individuals were affected, including 8 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Initiated incident protocols and reconfigured systems to prevent further unauthorized access. • Reported the incident to the United States Federal Bureau of Investigation. • Provided affected individuals with information to protect themselves from identity theft. • Reported the incident to payment card networks. • Took additional steps to increase security and management controls.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on June 3, 2016.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization did not specifically assess the harm that might result from this incident but provided affected individuals with information to protect themselves from identity theft and fraud. In my view, the financial information at issue could be used to cause the harms of identity theft and fraud. These are significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported that "…the test for reporting to the Commissioner is met, given the nature of the data and the circumstances". Further, the Organization "is of the view that individual notification is the right thing to do." I agree with the Organization's assessment. The likelihood of harm is increased as the incident resulted from malicious intent (deliberate intrusion), and the information was exposed for over one year. The information has not been recovered.

DECISION UNDER SECTION 37.1(1) OF PIPA
Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals. The financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm is increased as the incident resulted from malicious intent (deliberate intrusion), and the information was exposed for over one year. The information has not been recovered. I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified the affected individuals by letter on June 3, 2016. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner